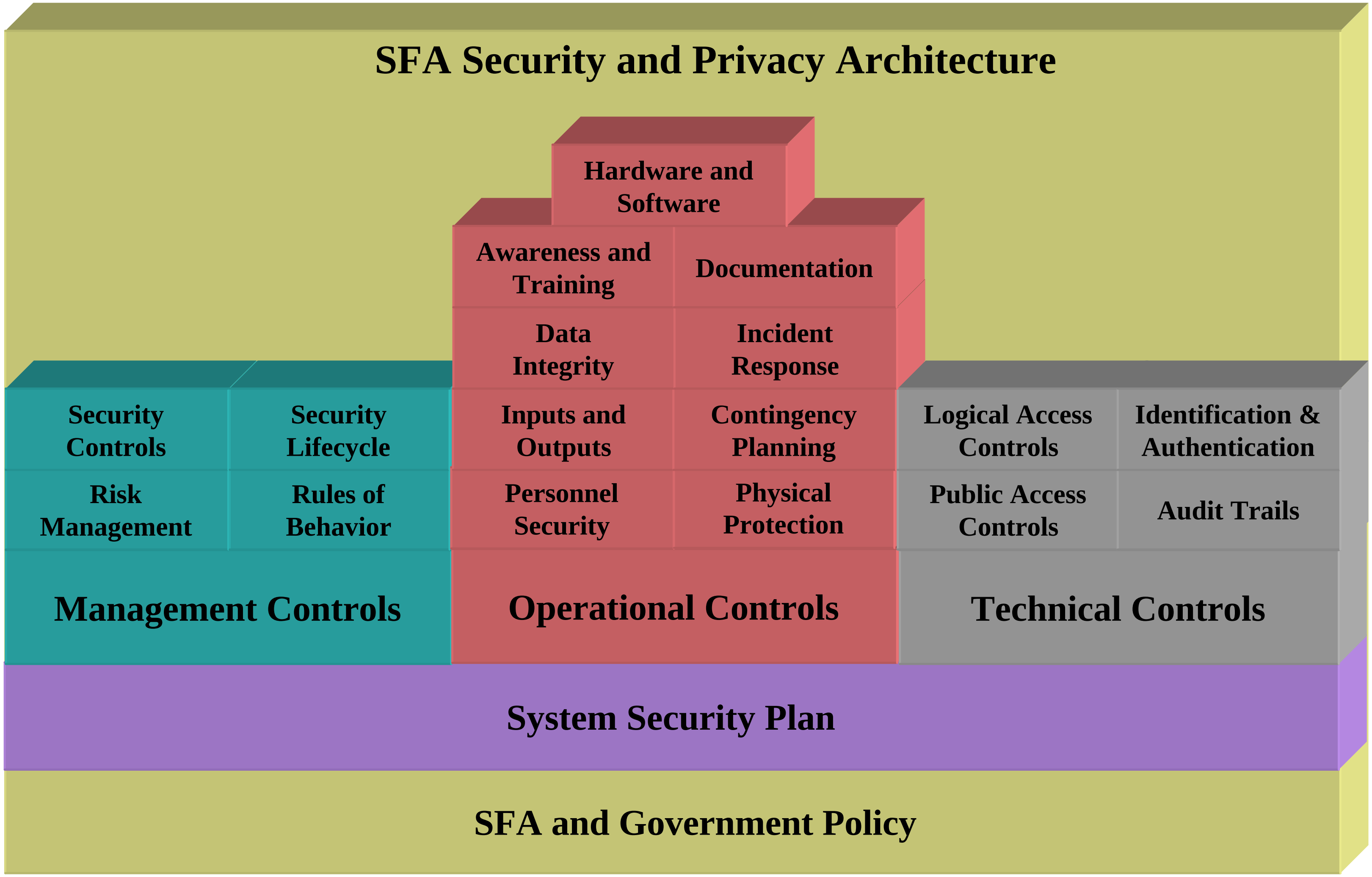
KPMG Consulting

PUBLIC SERVICES

SFA Modernization Project

September 13, 2001

Security and Privacy Architecture



SFA Security and Privacy Architecture

Hardware and Software

Awareness and Training

Documentation

Data Integrity

Incident Response

Inputs and Outputs

Contingency Planning

Personnel Security

Physical Protection

Security Controls

Security Lifecycle

Risk Management

Rules of Behavior

Logical Access Controls

Identification & Authentication

Public Access Controls

Audit Trails

Management Controls

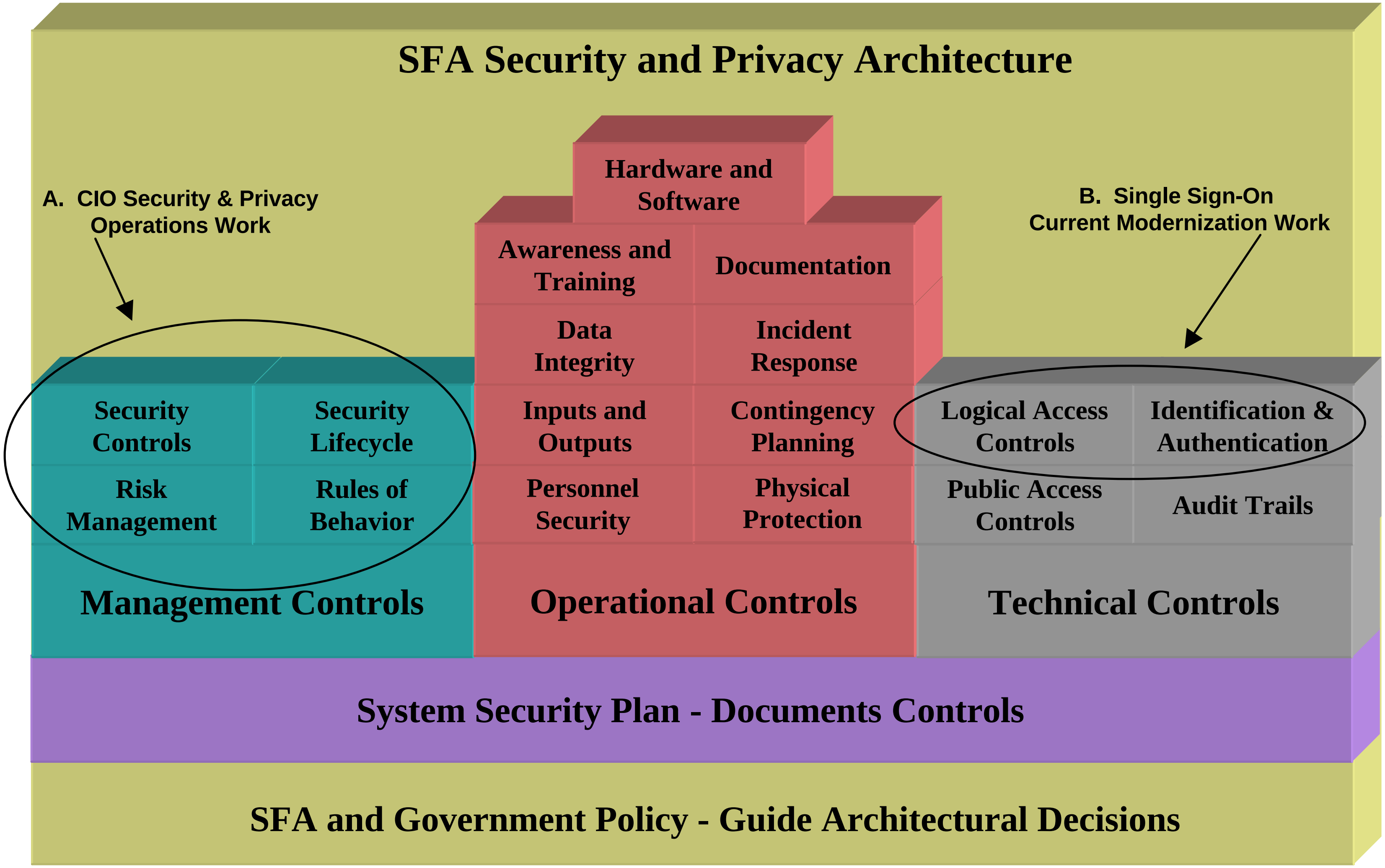
Operational Controls

Technical Controls

System Security Plan

SFA and Government Policy

Security and Privacy Architecture



SFA Security and Privacy Architecture

A. CIO Security & Privacy Operations Work

B. Single Sign-On Current Modernization Work

Hardware and Software

Awareness and Training

Documentation

Data Integrity

Incident Response

Security Controls

Security Lifecycle

Inputs and Outputs

Contingency Planning

Logical Access Controls

Identification & Authentication

Risk Management

Rules of Behavior

Personnel Security

Physical Protection

Public Access Controls

Audit Trails

Management Controls

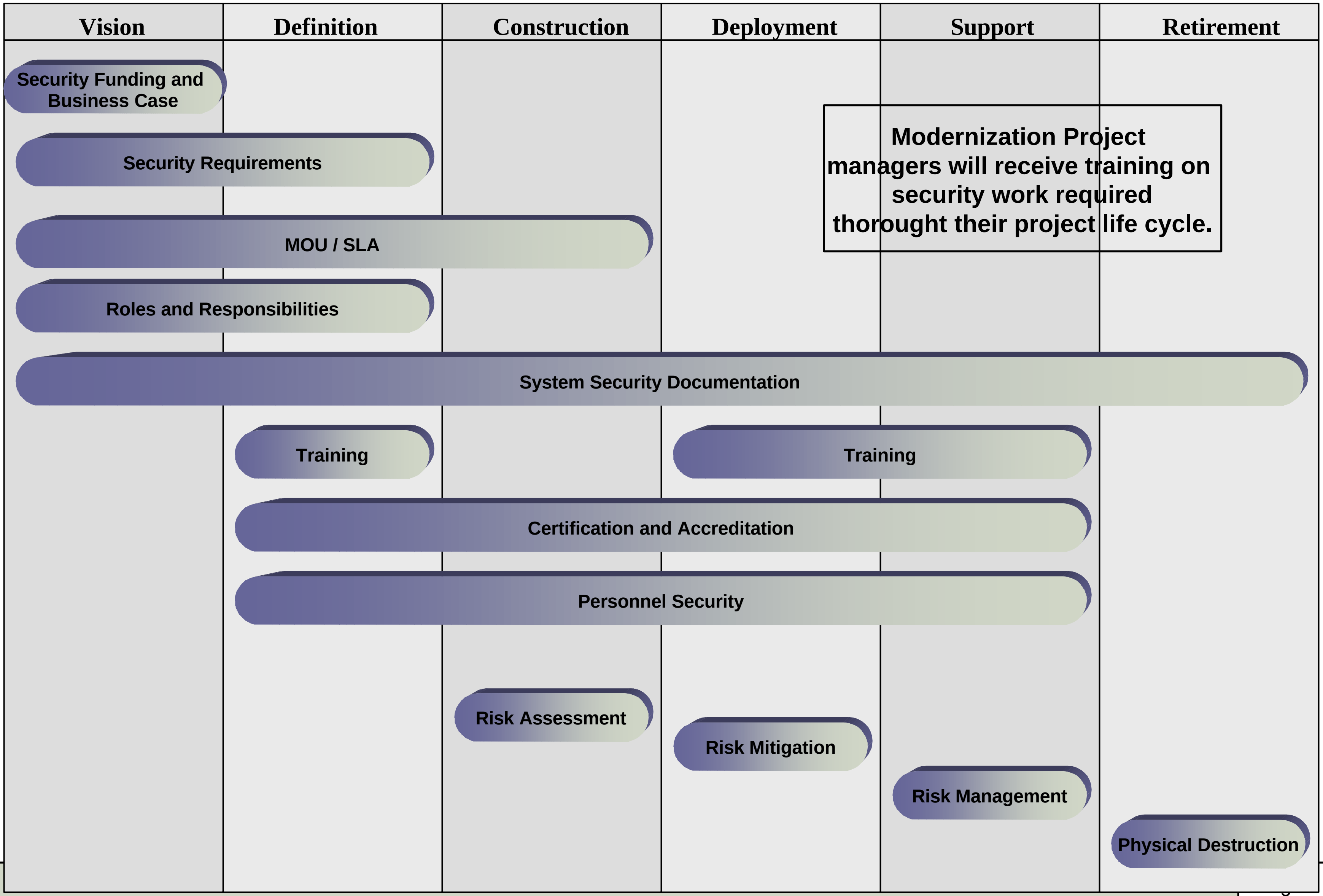
Operational Controls

Technical Controls

System Security Plan - Documents Controls

SFA and Government Policy - Guide Architectural Decisions

A. SDLC Security Components



Vision | Definition | Construction | Deployment | Support | Retirement

Security Funding and Business Case

Security Requirements

MOU / SLA

Roles and Responsibilities

System Security Documentation

Training

Training

Certification and Accreditation

Personnel Security

Risk Assessment

Risk Mitigation

Risk Management

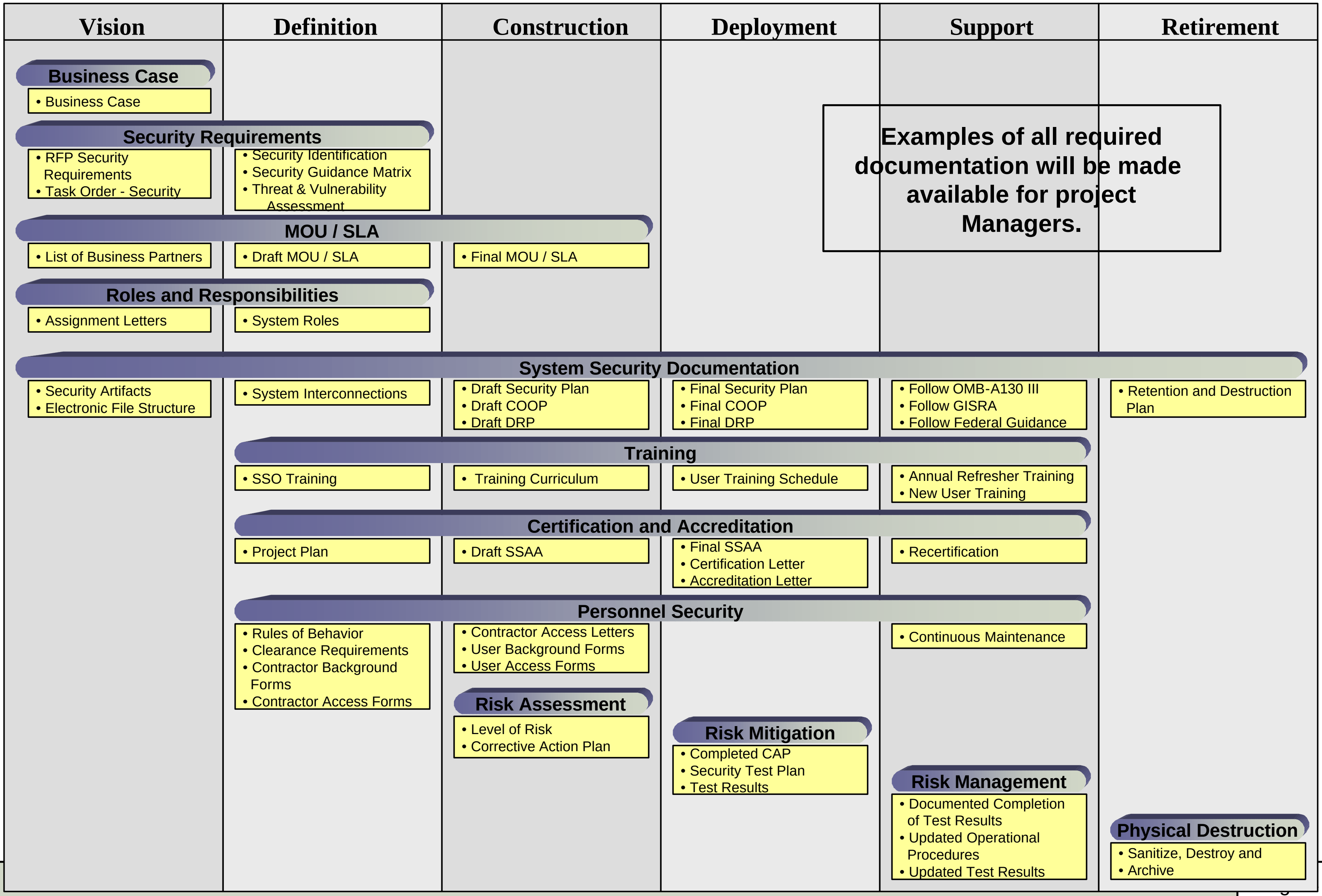
Physical Destruction

Modernization Project managers will receive training on security work required thorought their project life cycle.

A. SDLC Security Deliverables

KPMG Consulting

PUBLIC SERVICES



	Vision	Definition	Construction	Deployment	Support	Retirement
Business Case	• Business Case					
Security Requirements	• RFP Security Requirements • Task Order - Security	• Security Identification • Security Guidance Matrix • Threat & Vulnerability Assessment				
MOU / SLA	• List of Business Partners	• Draft MOU / SLA	• Final MOU / SLA			
Roles and Responsibilities	• Assignment Letters	• System Roles				
System Security Documentation	• Security Artifacts • Electronic File Structure	• System Interconnections	• Draft Security Plan • Draft COOP • Draft DRP	• Final Security Plan • Final COOP • Final DRP	• Follow OMB-A130 III • Follow GISRA • Follow Federal Guidance	• Retention and Destruction Plan
Training		• SSO Training	• Training Curriculum	• User Training Schedule	• Annual Refresher Training • New User Training	
Certification and Accreditation		• Project Plan	• Draft SSAA	• Final SSAA • Certification Letter • Accreditation Letter	• Recertification	
Personnel Security		• Rules of Behavior • Clearance Requirements • Contractor Background Forms • Contractor Access Forms	• Contractor Access Letters • User Background Forms • User Access Forms		• Continuous Maintenance	
Risk Assessment			• Level of Risk • Corrective Action Plan			
Risk Mitigation				• Completed CAP • Security Test Plan • Test Results		
Risk Management					• Documented Completion of Test Results • Updated Operational Procedures • Updated Test Results	
Physical Destruction						• Sanitize, Destroy and • Archive

Examples of all required documentation will be made available for project Managers.

B. Access Control Technology

Single Sign-On is a function of Access Control Technology (ACT). This is current Modernization Work on the Placemat.

□***Here are my credentials.***

The process of presenting a unique identifier to an information resource.

□***Do you recognize me?***

The process of verifying the user log on credentials.

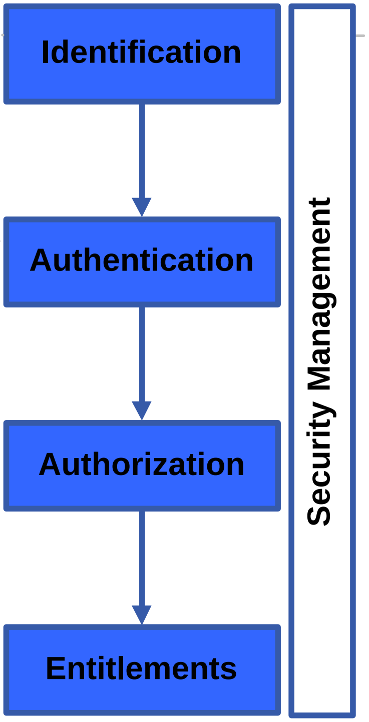
□***What systems and services can I access?***

Attributes assigned to a user account that indicate what systems, applications and services the user can access.

□***What can I do in those services?***

Access privileges assigned to a user account that allow the user to perform desired actions, such as View, Create, Modify, Delete or Enroll.

Access Control Technology (ACT)



□***How do I enroll for new services?***

- □ Potential area for significant savings.

□***What do I do if I cannot access my account?***

- □ A single group could be made responsible for administration of user accounts, currently dispersed across SFA business units.
- □ Individuals should have self-service capability to increase satisfaction and decrease administration cost.

Our Modernization Project has focused on building ACT as a re-usable service across the enterprise. The Single Sign-On Project for the Schools Portal is the first attempt to normalize sign-ons and increase user satisfaction.

B. Access Control Components

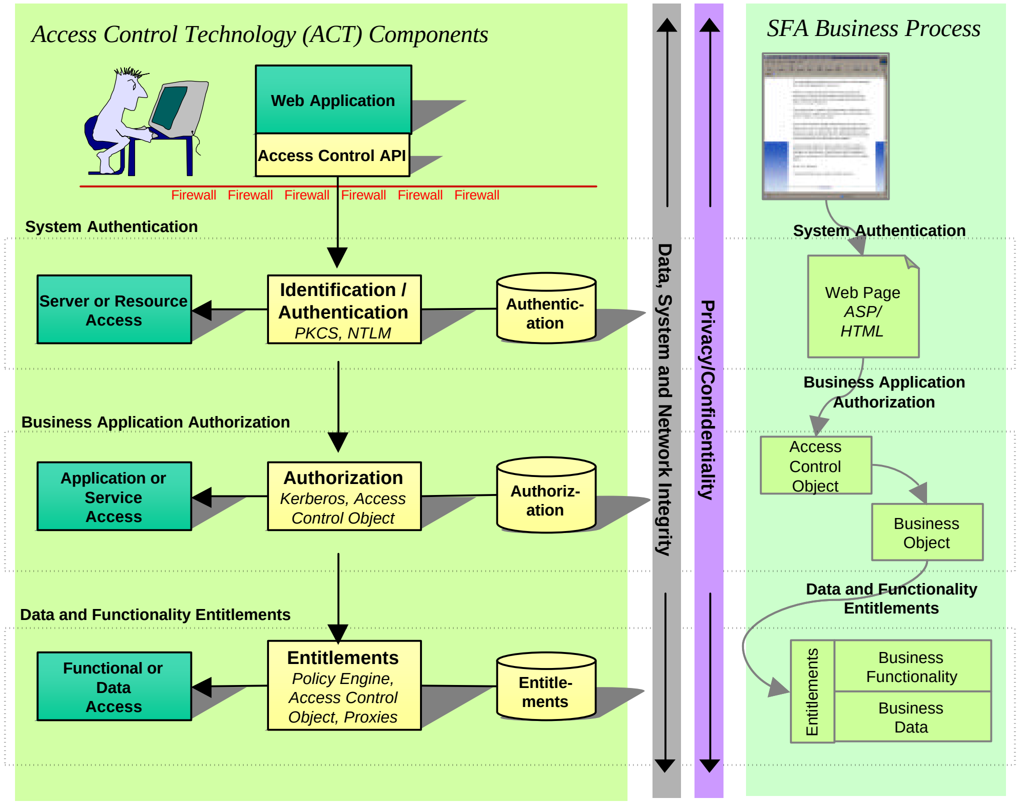
KPMG Consulting

PUBLIC SERVICES

- ACT manages how you access services, accounts, resources and data. An individual's identity is authenticated and the authenticated identity is used to determine what resources, services and information the individual can access.
- This is a tiered mechanism that can protect a systems environment at many different levels, including:
  - **Granting access to a web server**
  - **Restricting which accounts can be acted on**
  - **Defining what services are available**
  - **Further refining actions that can be executed within a service**

Access control will be administered by both SFA and trusted partners.

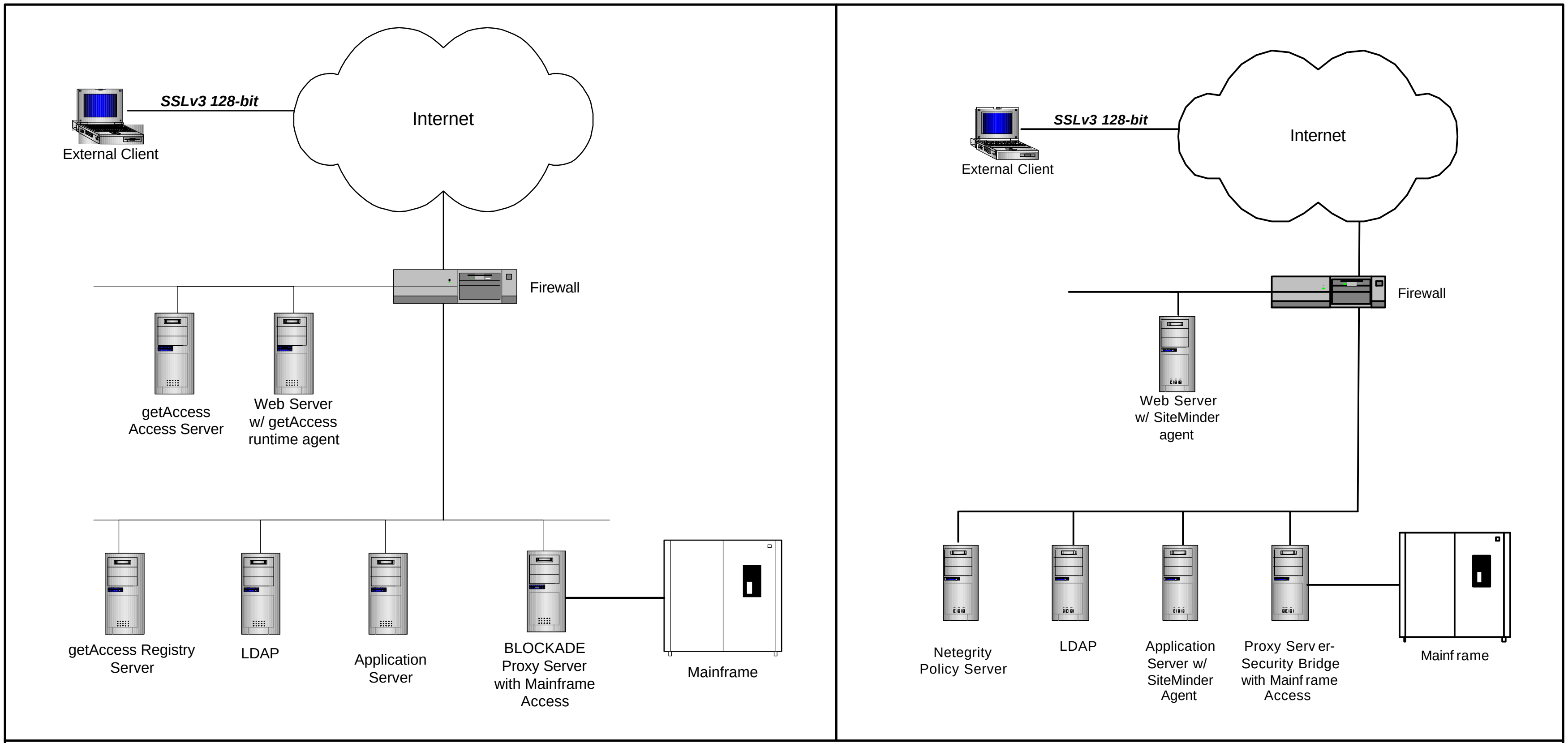
User enrollment and management could be centralized to create a share in savings opportunity. (But someone will lose their current business opportunity.)



Access Control Technology (ACT) Components
Web Application
Access Control API
Firewall Firewall Firewall Firewall Firewall Firewall
System Authentication
Server or Resource Access
Identification / Authentication
PKCS, NTLM
Authentic-ation
Business Application Authorization
Application or Service Access
Authorization
Kerberos, Access Control Object
Authoriz-ation
Data and Functionality Entitlements
Functional or Data Access
Entitlements
Policy Engine, Access Control Object, Proxies
Entitle-ments
Data, System and Network Integrity
Privacy/Confidentiality
SFA Business Process
System Authentication
Web Page
ASP/
HTML
Business Application Authorization
Access Control Object
Business Object
Data and Functionality Entitlements
Entitlements
Business Functionality
Business Data

B. ACT Implementation at SFA

Our work on Single Sign On has brought forward three findings that we did not know before: 1) User IDs must be normalized across applications; 2) A directory service is most often used to normalize IDs; and 3) SFA needs to cross business channels and assign ACT to one manager (CIO?).



Two Sample Vendor Solution Designs Considered for Single Sign-On at SFA